CLAIMS

What is claimed is:

1. An automation security system, comprising:

a factory protocol to transport data among end points of a communication channel; and

at least one security field associated with the factory protocol to authenticate at least one of a requestor of the data and a supplier of the data.

2. The system of claim 1, the security field further comprises path information to at least one of identify a requester/supplier of a connection, authenticate the requestor, and/or authenticate the supplier.

3. The system of claim 2, the path information facilitates non-connected data access by sending out an open-ended message.

4. The system of claim 1, the end points include at least one automation asset, the automation asset includes at least one of a controller, a communications module, a computer, a sensor actuator, a network sensor, an I/O device, a Human Machine Interface (HMI), an I/O module, and a network device.

5. The system of claim 1, the network communications channel is established across at least one of a control network, factory network, information network, private network, instrumentation network, a wireless network, and a public network.

6. The system of claim 1, further comprising at least one of a performance parameter and a security parameter in order to utilize the factory protocol.

7. The system of claim 6, further comprising employing weak encryption protocols for real time performance and strong security protocols for added security.

8. The system of claim 6, further comprising dynamically adjusting the factory protocol in accordance with at least one of the performance parameter and the security parameter.

9. The system of claim 1, the factory protocol including at least one of a time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, and a dynamic security adjustment field.

10. The system of claim 1, the factory protocol is adapted to at least one of a Control and Information Protocol (CIP) and .an object model that protects configuration of and transport of data between intelligent devices.

11. The system of claim 1, further comprising a component to at least one of provide source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, and provide refresh security protocols.

12. The system of claim 1, the factory protocol facilitates at least one of an identification, an authentication, an authorization, and a ciphersuite negotiation to establish network trusts.

13. The system of claim 1, the factory protocol is associated with a protocol supporting at least one of a Temporal Key Interchange Protocol (TKIP) and a wireless protocol.

14. The system of claim 1, the protocol employing at least one of an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller-Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPeCT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol and a Cellular Digital Packet Data (CDPD) protocol.

15. The system of claim 1, the network communications channel employing at least one of a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet network , an Ethernet network , DH/DH+ network , a Remote I/O network, a Fieldbus network, a Modbus network, a Profibus network.

16. The system of claim 1, further comprising a security field to limit access based upon line of sight parameters.

17. A method to facilitate factory automation network security, comprising:

determining network security requirements for an industrial automation system;

adapting a wireless security protocol to the industrial automation system; and

employing the wireless security protocol to communicate with the industrial automation system.

18. The method of claim 17, further comprising encapsulating an automation protocol in a TKIP protocol.

19. The method of claim 17, further comprising utilizing at least one of a Temporal Key Interchange Protocol (TKIP) and an Elliptical function in the wireless security protocol.

20. A method to facilitate automation network security, comprising:

establishing a communications session with an automation asset *via* a strong security protocol; and

exchanging data with the automation asset in accordance with real time communications *via* a lightweight security protocol that induces minimal impact on a system's performance.

21. The method of claim 20, further comprising dynamically switching between the extended security protocol and the lightweight security protocol during the real time communications.

22. The method of claim 20, the lightweight security protocol includes at least one of time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, and a dynamic security adjustment field.

23. The method of claim 20, the path component further comprising a component to identify a requestor of data.

24. An automation security system, comprising:

means for encoding a security component within a factory protocol;

means for transmitting the security component and the factory protocol across a network; and

means for decoding the security component in order to facilitate a secure communications channel across the network.

25. An automation security system, comprising:

an automation device adapted for network communications;

a factory protocol utilized by the automation device for network communications; and

an intrusion detection component adapted for the factory protocol to detect network attacks directed to the automation device.

26. The system of claim 25, the intrusion detection component is at least one of a host-based component and a network-based component.

27. The system of claim 25, the intrusion detection component is adapted to at least one of an attack signature, an address, an address range, a counter, a location, a time, an event, a control list, a virus and a Trojan executable.

28. A security violation detection methodology, comprising:

adapting an industrial network protocol in accordance with an intrusion detection technology; and

monitoring the industrial network protocol for an attack *via* the intrusion detection technology.

29. The method of claim 28, further comprising monitoring a network for flooding attacks.

30. The method of claim 28, further comprising:

detecting the attack protocol; and

automatically performing a security action after detecting the attack protocol.

31. The method of claim 30, the security action further comprising at least one of enabling an alarm, denying network access to the attack protocol, and removing a virus or an executable from a factory device.